Securing Downlink Non-Orthogonal Multiple Access Systems by Trusted Relays

Ahmed Arafa\textsuperscript{1}   Wonjae Shin\textsuperscript{2,1}   Mojtaba Vaezi\textsuperscript{3}   H. Vincent Poor\textsuperscript{1}

\textsuperscript{1}Electrical Engineering Department, Princeton University, USA
\textsuperscript{2}Department of Electronics Engineering, Pusan National University, South Korea
\textsuperscript{3}Electrical and Computer Engineering Department, Villanova University, USA

12/10/2018
Non-Orthogonal Multiple Access (NOMA)

- NOMA techniques offer solutions to spectrum scarcity and congestion problems.

- **Key feature:** efficient utilization of available resources serving multiple users simultaneously over the same resource: frequency, time, code, or space.

- Vulnerable to eavesdropping (wireless communications inherent openness).

- How to provide security guarantees with multiple interfering users?
Security at the Physical Layer

- Traditionally a higher-layer issue: encryption, key distribution.
- Might be insufficient with the increasing computational powers of adversarial nodes/eavesdroppers.

- **Physical layer security** provides security by exploiting the imperfections in the physical communication channel: noise, fading, interference.
- Joint encoding for security and reliability.
Physical Layer Security for NOMA—Related Works

- **SISO** secrecy sum rate maximization: [Zhang - Wang - Yang - Ding '16].

- **Large-scale** security for downlink: [liu - Qin - Elkashlan - Gao - Hanzo '17]; and uplink: [Gomez - Martin-Vega - Lopez-Martinez - Liu - Elkashlan '17].

- NOMA-assisted **multicast-unicast** streaming: [Ding - Zhao - Peng - Poor '17].

- **MIMO** secrecy sum rate: [Tian - Zhang - Zhao - Li - Qin '17].

- One user is **untrusted** with MISO: [Li - Jiang - Zhang - Li - Qin '17]; and MIMO: [Jiang - Li - Zhang - Li - Qin '17].

- Transmit antenna selection: [Lei - Zhang - Park - Xu - Ansari - Pan - Alomair - Alouini '17].

- Secrecy rate maximization with **outage probability** constraints: [He - Liu - Yang - Lau '17].

- ...
BS uses superposition coding to send two messages to the legitimate users:

\[ x = \sqrt{\alpha P} s_1 + \sqrt{\bar{\alpha} P} s_2 \]

- **Strong** user decodes both messages using successive interference cancellation.
- **Weak** user decodes its message by treating interference as noise.
- An external **eavesdropper** wiretaps the communication.
Secrecy capacities of this multi-receiver wiretap channel [Ekrem-Ulukus ’11]:

\[ r_{s,1} = \left[ \log \left( 1 + |h_1|^2 \alpha P \right) - \log \left( 1 + |h_e|^2 \alpha P \right) \right]^+ \]

\[ r_{s,2} = \left[ \log \left( 1 + \frac{|h_2|^2 \bar{\alpha} P}{1 + |h_2|^2 \bar{\alpha} P} \right) - \log \left( 1 + \frac{|h_e|^2 \bar{\alpha} P}{1 + |h_e|^2 \bar{\alpha} P} \right) \right]^+ \]
How can a number of trusted cooperative relays enhance the secrecy rate region?
Channels are complex-valued, fixed, and known. Noise is $\sim \mathcal{CN}(0, 1)$.

$K$ relays, half-duplex, trusted, and cooperative.

Each node is equipped with a single-antenna (SISO).

BS reduces its power to $\bar{P}$; relays share the remaining $P - \bar{P}$.

Three relaying schemes: cooperative jamming, decode-and-forward and amplify-and-forward.
Relaying Scheme 1: Cooperative Jamming

- Relays transmit a **jamming** signal $Jz$ simultaneously with the BS’s transmission.
- $z \sim \mathcal{CN}(0, 1)$; $J \in \mathbb{C}^K$ is a **beamforming** vector.
- Jamming signal should not affect the legitimate users:

$$[g_1 \quad g_2]^\dagger J_o \triangleq G^\dagger J_o = \begin{bmatrix} 0 & 0 \end{bmatrix}$$
Without relays (direct transmission):

\[
    r_{s,1} = \left[ \log \left( 1 + |h_1|^2 \alpha P \right) - \log \left( 1 + |h_e|^2 \alpha P \right) \right]^+
\]

\[
    r_{s,2} = \left[ \log \left( 1 + \frac{|h_2|^2 \bar{\alpha} P}{1 + |h_2|^2 \alpha P} \right) - \log \left( 1 + \frac{|h_e|^2 \bar{\alpha} P}{1 + |h_e|^2 \alpha P} \right) \right]^+
\]
With cooperative jamming:

\[ r_{s,1}^J = \left[ \log \left( 1 + |h_1|^2 \bar{\alpha} \bar{P} \right) - \log \left( 1 + \frac{|h_e|^2 \bar{\alpha} \bar{P}}{1 + |g_e^\dagger J_o|^2} \right) \right]^+ \]

\[ r_{s,2}^J = \left[ \log \left( 1 + \frac{|h_2|^2 \bar{\alpha} \bar{P}}{1 + |h_2|^2 \bar{\alpha} \bar{P}} \right) - \log \left( 1 + \frac{|h_e|^2 \bar{\alpha} \bar{P}}{1 + |h_e|^2 \bar{\alpha} \bar{P} + |g_e^\dagger J_o|^2} \right) \right]^+ \]

**Best beamforming vector:**

\[
\max_{J_o} |g_e^\dagger J_o|^2 \\
\text{s.t. } G^\dagger J_o = [0 \ 0] \\
J_o^\dagger J_o = P - \bar{P}
\]

**Unique solution:**

\[
\hat{J}_o = \frac{\mathcal{P}^\perp(G) g_e}{\|\mathcal{P}^\perp(G) g_e\|} \sqrt{P - \bar{P}}
\]

\( \mathcal{P}^\perp(\cdot) \) is a projection matrix:

\[
\mathcal{P}^\perp(G) \triangleq I_K - G \left( G^\dagger G \right)^{-1} G^\dagger
\]
With cooperative jamming:

\[
r_{s,1}^J = \left[ \log \left( 1 + |h_1|^2 \alpha \bar{P} \right) - \log \left( 1 + \frac{|h_e|^2 \alpha \bar{P}}{1 + |g_e^\dagger J_o|^2} \right) \right]^+ \\
r_{s,2}^J = \left[ \log \left( 1 + \frac{|h_2|^2 \bar{\alpha} \bar{P}}{1 + |h_2|^2 \alpha \bar{P}} \right) - \log \left( 1 + \frac{|h_e|^2 \bar{\alpha} \bar{P}}{1 + |h_e|^2 \alpha \bar{P} + |g_e^\dagger J_o|^2} \right) \right]^+
\]

Best beamforming vector:

\[
\max_{J_o} \quad |g_e^\dagger J_o|^2 \\
\text{s.t.} \quad G^\dagger J_o = [0 \ 0] \\
J_o^\dagger J_o = P - \bar{P}
\]

Unique solution:

\[
\hat{J}_o = \frac{\mathcal{P}(G) g_e}{\|\mathcal{P}(G) g_e\|} \sqrt{P - \bar{P}}
\]

\(\mathcal{P}(\cdot)\) is a projection matrix:

\[
\mathcal{P}(G) \triangleq I_K - G (G^\dagger G)^{-1} G^\dagger
\]
With cooperative jamming:

\[
\begin{align*}
    r_{s,1}^J &= \left[ \log \left( 1 + |h_1|^2 \alpha \bar{P} \right) - \log \left( 1 + \frac{|h_e|^2 \alpha \bar{P}}{1 + |g^\dagger J_o|^2} \right) \right]^+ \\
    r_{s,2}^J &= \left[ \log \left( 1 + \frac{|h_2|^2 \alpha \bar{P}}{1 + |h_2|^2 \alpha \bar{P}} \right) - \log \left( 1 + \frac{|h_e|^2 \alpha \bar{P}}{1 + |h_e|^2 \alpha \bar{P} + |g^\dagger J_o|^2} \right) \right]^+
\end{align*}
\]

Best beamforming vector:

\[
\max_{J_o} \quad |g^\dagger J_o|^2 \\
\text{s.t.} \quad G^\dagger J_o = [0 \quad 0] \\
\quad J_o^\dagger J_o = P - \bar{P}
\]

Unique solution:

\[
\hat{J}_o = \frac{P \perp (G) g_e}{\|P \perp (G) g_e\|} \sqrt{P - \bar{P}}
\]

\(P \perp (\cdot)\) is a projection matrix:

\[
P \perp (G) \triangleq I_K - G \left( G^\dagger G \right)^{-1} G^\dagger
\]
Relaying Scheme 2: Decode-and-Forward

Communication occurs over two phases:

1. **Phase 1**: BS broadcasts the messages to both relays and legitimate users.
2. **Phase 2**: Relays decode, forward toward users via superposition coding, and use a beamforming vector $d \in \mathbb{C}^K$.

In what order should the $k$th relay decode? *Depends on operating point*...

1. **(1): strong user’s message first**:
   
   $$ R_{k,1}^{(1)} = \log \left( 1 + \frac{|h_{r,k}|^2 \alpha \bar{P}}{1 + |h_{r,k}|^2 \bar{\alpha} \bar{P}} \right) $$
   
   $$ R_{k,2}^{(1)} = \log \left( 1 + |h_{r,k}|^2 \bar{\alpha} \bar{P} \right) $$

2. **(2): weak user’s message first**:
   
   $$ R_{k,1}^{(2)} = \log \left( 1 + |h_{r,k}|^2 \alpha \bar{P} \right) $$
   
   $$ R_{k,2}^{(2)} = \log \left( 1 + \frac{|h_{r,k}|^2 \bar{\alpha} \bar{P}}{1 + |h_{r,k}|^2 \alpha \bar{P}} \right) $$
Relaying Scheme 2: Decode-and-Forward

Communication occurs over two phases:

- **Phase 1**: BS broadcasts the messages to both relays and legitimate users.
- **Phase 2**: Relays decode, forward toward users via superposition coding, and use a beamforming vector $d \in \mathbb{C}^K$.

In what order should the $k$th relay decode? Depends on operating point...

1. **Strong user's message first**:
   \[
   R_{k,1}^{(1)} = \log \left( 1 + \frac{|h_{r,k}|^2 \alpha \bar{P}}{1 + |h_{r,k}|^2 \bar{\alpha} \bar{P}} \right)
   \]
   \[
   R_{k,2}^{(1)} = \log \left( 1 + |h_{r,k}|^2 \bar{\alpha} \bar{P} \right)
   \]

2. **Weak user's message first**:
   \[
   R_{k,1}^{(2)} = \log \left( 1 + |h_{r,k}|^2 \alpha \bar{P} \right)
   \]
   \[
   R_{k,2}^{(2)} = \log \left( 1 + \frac{|h_{r,k}|^2 \bar{\alpha} \bar{P}}{1 + |h_{r,k}|^2 \alpha \bar{P}} \right)
   \]
Relaying Scheme 2: Decode-and-Forward

- Communication occurs over two phases:
  - **Phase 1**: BS broadcasts the messages to both relays and legitimate users.
  - **Phase 2**: Relays decode, forward toward users via superposition coding, and use a beamforming vector $d \in \mathbb{C}^K$.

- In what order should the $k$th relay decode? *Depends on operating point*...

1. **(1): strong user’s message first:**
   \[
   R_{k,1}^{(1)} = \log \left( 1 + \frac{|h_{r,k}|^2 \alpha \bar{P}}{1 + |h_{r,k}|^2 \bar{\alpha} \bar{P}} \right) \\
   R_{k,2}^{(1)} = \log (1 + |h_{r,k}|^2 \bar{\alpha} \bar{P})
   \]

2. **(2): weak user’s message first:**
   \[
   R_{k,1}^{(2)} = \log (1 + |h_{r,k}|^2 \alpha \bar{P}) \\
   R_{k,2}^{(2)} = \log \left( 1 + \frac{|h_{r,k}|^2 \bar{\alpha} \bar{P}}{1 + |h_{r,k}|^2 \alpha \bar{P}} \right)
   \]
Relaying Scheme 2: Decode-and-Forward

Communication occurs over two phases:

**Phase 1:** BS broadcasts the messages to both relays and legitimate users.

**Phase 2:** Relays decode, forward toward users via superposition coding, and use a beamforming vector $d \in \mathbb{C}^K$.

In what order should the $k$th relay decode? *Depends on operating point*...

1. **Strong user’s message first:**
   \[
   R_{k,1}^{(1)} = \log \left( 1 + \frac{|h_{r,k}|^2 \alpha \bar{P}}{1 + |h_{r,k}|^2 \alpha \bar{P}} \right) 
   \]
   \[
   R_{k,2}^{(1)} = \log \left( 1 + |h_{r,k}|^2 \alpha \bar{P} \right) 
   \]

2. **Weak user’s message first:**
   \[
   R_{k,1}^{(2)} = \log \left( 1 + |h_{r,k}|^2 \alpha \bar{P} \right) 
   \]
   \[
   R_{k,2}^{(2)} = \log \left( 1 + \frac{|h_{r,k}|^2 \alpha \bar{P}}{1 + |h_{r,k}|^2 \alpha \bar{P}} \right) 
   \]
Relaying Scheme 2: Decode-and-Forward

Communication occurs over two phases:

- **Phase 1**: BS broadcasts the messages to both relays and legitimate users.
- **Phase 2**: Relays decode, forward toward users via superposition coding, and use a beamforming vector $d \in \mathbb{C}^K$.

In what order should the $k$th relay decode? *Depends on operating point*...

- (1): strong user’s message first:
  
  $R_{k,1}^{(1)} = \log \left( 1 + \frac{|h_{r,k}|^2 \alpha \bar{P}}{1 + |h_{r,k}|^2 \bar{\alpha} \bar{P}} \right)$

  $R_{k,2}^{(1)} = \log \left( 1 + |h_{r,k}|^2 \bar{\alpha} \bar{P} \right)$

- (2): weak user’s message first:

  $R_{k,1}^{(2)} = \log \left( 1 + |h_{r,k}|^2 \alpha \bar{P} \right)$

  $R_{k,2}^{(2)} = \log \left( 1 + \frac{|h_{r,k}|^2 \bar{\alpha} \bar{P}}{1 + |h_{r,k}|^2 \alpha \bar{P}} \right)$
Communication occurs over two phases:

- **Phase 1**: BS broadcasts the messages to both relays and legitimate users.
- **Phase 2**: Relays decode, forward toward users via superposition coding, and use a beamforming vector $d \in \mathbb{C}^K$.

Eavesdropper overhears communication in both phases.

Eliminate eavesdropping benefit in **Phase 2**:

$$g_e^\dagger d_o = 0$$
Relaying Scheme 2: Decode-and-Forward

Communication occurs over two phases:

- **Phase 1**: BS broadcasts the messages to both relays and legitimate users.
- **Phase 2**: Relays decode, forward toward users via superposition coding, and use a beamforming vector $d \in \mathbb{C}^K$.

- Eavesdropper overhears communication in both phases.

- Eliminate eavesdropping benefit in **Phase 2**:
  \[ g_e^\dagger d_o = 0 \]
Without relays (direct transmission):

\[ r_{s,1} = \left[ \log \left( 1 + |h_1|^2 \alpha P \right) - \log \left( 1 + |h_e|^2 \alpha P \right) \right]^+ \]

\[ r_{s,2} = \left[ \log \left( 1 + \frac{|h_2|^2 \bar{\alpha} P}{1 + |h_2|^2 \alpha P} \right) - \log \left( 1 + \frac{|h_e|^2 \bar{\alpha} P}{1 + |h_e|^2 \alpha P} \right) \right]^+ \]
Relaying Scheme 2: Decode-and-Forward—Achievable Secrecy Rates

- With decode-and-forward:

\[
\begin{align*}
    r_{s,1}^{DF} &= \frac{1}{2} \left[ r_1^{DF} - \log \left( 1 + |h_e|^2 \alpha \bar{P} \right) \right]^+ \\
    r_{s,2}^{DF} &= \frac{1}{2} \left[ r_2^{DF} - \log \left( 1 + \frac{|h_e|^2 \alpha \bar{P}}{1 + |h_e|^2 \alpha \bar{P}} \right) \right]^+ \\
\end{align*}
\]

where

\[
\begin{align*}
    r_1^{DF} &= \min \left\{ \log \left( 1 + |h_1|^2 \alpha \bar{P} \right) + \log \left( 1 + |g_1^\dagger d_o|^2 \alpha (P - \bar{P}) \right), \min_{1 \leq k \leq K} R_{k,1}^{(i)} \right\} \\
    r_2^{DF} &= \min \left\{ \log \left( 1 + \frac{|h_2|^2 \alpha \bar{P}}{1 + |h_2|^2 \alpha \bar{P}} \right) + \log \left( 1 + \frac{|g_2^\dagger d_o|^2 \alpha (P - \bar{P})}{1 + |g_2^\dagger d_o|^2 \alpha (P - \bar{P})} \right), \min_{1 \leq k \leq K} R_{k,2}^{(i)} \right\} \\
\end{align*}
\]

- Secrecy rates depend on decoding order \((i), i = 1, 2\), at the relays.

- Extra \(\frac{1}{2}\) terms are due to sending same information over two phases.
Relaying Scheme 2: Decode-and-Forward—Achievable Secrecy Rates

With decode-and-forward:

\[
\begin{align*}
    r_{s,1}^{DF} &= \frac{1}{2} \left[ r_1^{DF} - \log \left( 1 + |h_e|^2 \bar{\alpha} \bar{P} \right) \right]^+ \\
    r_{s,2}^{DF} &= \frac{1}{2} \left[ r_2^{DF} - \log \left( 1 + \frac{|h_e|^2 \bar{\alpha} \bar{P}}{1 + |h_e|^2 \alpha \bar{P}} \right) \right]^+
\end{align*}
\]

where

\[
\begin{align*}
    r_1^{DF} &= \min \left\{ \log \left( 1 + |h_1|^2 \alpha \bar{P} \right) + \log \left( 1 + |g_1^\dagger d_o|^2 \alpha (P - \bar{P}) \right), \min_{1 \leq k \leq K} R_{k,1}^{(i)} \right\} \\
    r_2^{DF} &= \min \left\{ \log \left( 1 + \frac{|h_2|^2 \bar{\alpha} \bar{P}}{1 + |h_2|^2 \alpha \bar{P}} \right) + \log \left( 1 + \frac{|g_2^\dagger d_o|^2 \bar{\alpha} (P - \bar{P})}{1 + |g_2^\dagger d_o|^2 \alpha (P - \bar{P})} \right), \min_{1 \leq k \leq K} R_{k,2}^{(i)} \right\}
\end{align*}
\]

- Fix \(0 \leq \beta \leq 1\).
- Proposed beamforming vector:

\[
\begin{align*}
    \max_{d_o} \quad & \beta \left| g_1^\dagger d_o \right|^2 + (1 - \beta) \left| g_2^\dagger d_o \right|^2 \\
    \text{s.t.} \quad & g_e^\dagger d_o = 0 \\
    & d_o^\dagger d_o = 1
\end{align*}
\]

- Unique solution:

\[
\begin{align*}
    \hat{d}_o &= \frac{\mathcal{P}^\perp(g_e) \hat{u}_d}{\|\mathcal{P}^\perp(g_e) \hat{u}_d\|} \\
    \hat{u}_d &= \text{leading eigenvector of } \mathcal{P}^\perp(g_e) \left( \beta g_1 g_1^\dagger + (1 - \beta) g_2 g_2^\dagger \right) \mathcal{P}^\perp(g_e)
\end{align*}
\]
Relaying Scheme 2: Decode-and-Forward—Achievable Secrecy Rates

- With decode-and-forward:

\[
\begin{align*}
    r_{s,1}^{DF} &= \frac{1}{2} \left[ r_1^{DF} - \log \left( 1 + |h_e|^2 \alpha \bar{P} \right) \right]^+ \\
    r_{s,2}^{DF} &= \frac{1}{2} \left[ r_2^{DF} - \log \left( 1 + \frac{|h_e|^2 \bar{\alpha} \bar{P}}{1 + |h_e|^2 \alpha \bar{P}} \right) \right]^+ 
\end{align*}
\]

where

\[
\begin{align*}
    r_1^{DF} &= \min \left\{ \log (1 + |h_1|^2 \alpha \bar{P}) + \log \left( 1 + |g_1^\dagger d_o|^2 \alpha (P - \bar{P}) \right), \min_{1 \leq k \leq K} R_{k,1}^{(i)} \right\} \\
    r_2^{DF} &= \min \left\{ \log \left( 1 + \frac{|h_2|^2 \bar{\alpha} \bar{P}}{1 + |h_2|^2 \alpha \bar{P}} \right) + \log \left( 1 + \frac{|g_2^\dagger d_o|^2 \bar{\alpha} (P - \bar{P})}{1 + |g_2^\dagger d_o|^2 \alpha (P - \bar{P})} \right), \min_{1 \leq k \leq K} R_{k,2}^{(i)} \right\} 
\end{align*}
\]

- Fix \(0 \leq \beta \leq 1\).

- Proposed beamforming vector:

\[
\begin{align*}
    \max_{d_o} & \quad \beta |g_1^\dagger d_o|^2 + (1 - \beta) |g_2^\dagger d_o|^2 \\
\text{s.t.} & \quad g_e^\dagger d_o = 0 \\
& \quad d_o^\dagger d_o = 1
\end{align*}
\]

- Unique solution:

\[
\hat{d}_o = \frac{\mathcal{P}^\perp(g_e) \hat{u}_d}{\|\mathcal{P}^\perp(g_e) \hat{u}_d\|}
\]

- \(\hat{u}_d\): leading eigenvector of

\[
\mathcal{P}^\perp(g_e) \left( \beta g_1 g_1^\dagger + (1 - \beta) g_2 g_2^\dagger \right) \mathcal{P}^\perp(g_e)
\]
Communication also occurs over two phases:

- **Phase 1**: BS broadcasts the messages to both relays and legitimate users.
- **Phase 2**: Relays multiply their received signal $y_r$ by a beamforming vector $a \in \mathbb{C}^K$ and forward to users.

Eavesdropper overhears communication in both phases.

Eliminate eavesdropping benefit in **Phase 2**:

$$g_e \mathop{\dagger} \text{diag}(h_r) a_o = 0$$
Communication also occurs over two phases:

- **Phase 1**: BS broadcasts the messages to both relays and legitimate users.
- **Phase 2**: Relays multiply their received signal $y_r$ by a beamforming vector $a \in \mathbb{C}^K$ and forward to users.

Eavesdropper overhears communication in both phases.

Eliminate eavesdropping benefit in **Phase 2**:

$$g_e^\dagger \text{diag}(h_r) a_o = 0$$
Communication also occurs over two phases:

- **Phase 1**: BS broadcasts the messages to both relays and legitimate users.
- **Phase 2**: Relays multiply their received signal $y_r$ by a beamforming vector $a \in \mathbb{C}^K$ and forward to users.

Eavesdropper overhears communication in both phases.

Eliminate eavesdropping benefit in **Phase 2**:

$$g_e^\dagger \text{diag}(h_r) a_o = 0$$
Relaying Scheme 3: Amplify-and-Forward—Achievable Secrecy Rates

Without relays (direct transmission):

\[ r_{s,1} = \left[ \log \left( 1 + |h_1|^2 \alpha P \right) - \log \left( 1 + |h_e|^2 \alpha P \right) \right]^+ \]

\[ r_{s,2} = \left[ \log \left( 1 + \frac{|h_2|^2 \bar{\alpha} P}{1 + |h_2|^2 \alpha P} \right) - \log \left( 1 + \frac{|h_e|^2 \bar{\alpha} P}{1 + |h_e|^2 \alpha P} \right) \right]^+ \]
Relaying Scheme 3: Amplify-and-Forward—Achievable Secrecy Rates

With amplify-and-forward:

\[
\begin{align*}
    r_{s,1}^{AF} &= \frac{1}{2} \left[ \log \left( 1 + |h_1|^2 \alpha \bar{P} + \frac{a_o^\dagger G_{1,r} a_o}{1 + a_o^\dagger G_1 a_o} \alpha \bar{P} \right) - \log \left( 1 + |h_e|^2 \alpha \bar{P} \right) \right]^+ \\
    r_{s,2}^{AF} &= \frac{1}{2} \left[ \log \left( 1 + \frac{|h_2|^2 \alpha \bar{P}}{1 + |h_2|^2 \alpha \bar{P}} + \frac{a_o^\dagger G_{2,r} a_o \alpha \bar{P}}{1 + a_o^\dagger G_2 a_o + a_o^\dagger G_{2,r} a_o \alpha \bar{P}} \right) - \log \left( 1 + \frac{|h_e|^2 (1 - \alpha) \bar{P}}{1 + |h_e|^2 \alpha \bar{P}} \right) \right]^+ \\
\end{align*}
\]

where

\[
G_{j,r} \triangleq \text{diag}(h_r^*) g_j g_j^\dagger \text{diag}(h_r), \quad j = 1, 2
\]
\[
G_j \triangleq \text{diag}(g_j^*) \text{diag}(g_j), \quad j = 1, 2
\]

Extra \( \frac{1}{2} \) terms are due to sending same information over two phases.
Best beamforming vector for $j$th user:

$$a_o^{(j)} = \sqrt{\frac{P - \bar{P}}{u_a^{(j)T} F A F u_a^{(j)}}} F u_a^{(j)}$$

where

$$F \triangleq \mathcal{P}^\perp (\text{diag}(h_r) g_e)$$

$$A \triangleq (\text{diag}(h_r^*) \text{diag}(h_r) \bar{P} + I_K)$$

$u_a^{(1)}$: leading generalized eigenvector of

$$\left( FG_{1,r} F , F \left( \frac{1}{P - \bar{P}} A + G_1 \right) F \right)$$

$u_a^{(2)}$: leading generalized eigenvector of

$$\left( FG_{2,r} F , F \left( \frac{1}{P - \bar{P}} A + G_2 + G_{2,r} \alpha \bar{P} \right) F \right)$$

Fix $0 \leq \beta \leq 1$. Proposed beamforming vector:

$$\hat{a}_o = \beta a_o^{(1)} + (1 - \beta) a_o^{(2)}$$
Characterize the boundary of the secrecy rate region \((n \in \{J, DF, AF\})\):

\[
\max_{\alpha, \bar{P}} \mu r_{s,1}^n + (1 - \mu) r_{s,2}^n
\]

s.t. \(0 \leq \bar{P} \leq P\), \(0 \leq \alpha \leq 1\)

- \(K = 5\) relays.

- Pick \(\beta = \mu\) for decode-and-forward and amplify-and-forward beamforming vectors.

- Channel gain between two nodes: \(h = \sqrt{1/l^\gamma} e^{i\theta}\)
  - \(l\): distance between the two nodes.
  - \(\gamma\): path loss exponent.
  - \(\theta\): uniform random variable on \([0, 2\pi]\).
Dashed lines are when eavesdropper is in between BS and legitimate users; solid lines are when it is beyond them.
Dashed lines are when eavesdropper is in between BS and legitimate users; solid lines are when it is beyond them.
Dashed lines are when eavesdropper is in between BS and legitimate users; solid lines are when it is beyond them.
Considered the *relaying* benefits on physical layer security of a two-user SISO downlink NOMA with an external eavesdropper.

**Take-away message:** best relaying scheme depends on relative locations.

**Extensions:**
- Full-duplex relays.
- Eavesdropper’s channel is unknown.
- MIMO scenarios.
- Untrusted relays (presented at *Asilomar ’18*).
- ...